

January 10, 1997

Ms. Nancy Crowe  
Regulatory Policy Division  
Bureau of Export Administration  
Department of Commerce  
14th Street and Pennsylvania Ave, NW  
Room 2705  
Washington, D.C. 20230

Dear Ms. Crowe

Please consider the following comments re: **Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List.**

General Comment

The market place rather than Government regulation should drive the need for Key Recovery features. There are many reasons to suspect that the market judges Key Recovery as undesirable.

Supplement No. 4 to Part 742

The phrase "with a reasonable frequency" is vague and does not provide meaningful guidance. We suggest that the phrase be replaced by "at least every 24 hours".

The phrase "without requiring repeated presentations of access authorization to the key recovery agent(s)" presupposes a key escrow scheme. We suggest that phrase be replaced by "in a manner consistent with the requirements of Section III of Supplement No. 5 to Part 742."

Supplement No. 6 to Part 742

Calling out proprietary encryption algorithms, RC2 and RC4, constitutes an inhibition of fair trade by promoting use of proprietary algorithms subject to discretionary licensing fees imposed by a commercial entity. We urge the addition of 40-bit DES as well as any other public domain algorithm to the allowable algorithms.

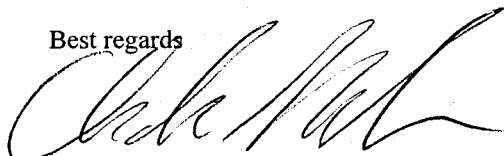
Sec 744.9

This clause is poorly written and self contradictory. For example, the first part prohibits training, but in the sentence beginning with "Note in addition ..." "teaching" and "discussions" are allowed. We suggest that the phrase "foreign person in the development or manufacture" be replaced by "foreign person in the development for manufacture".

If you require additional information or discussion, feel free to contact me at 408 774-2540 or [cwilliams@cylink.com](mailto:cwilliams@cylink.com).

Cylink Corporation is the leading supplier of data security solutions throughout the world. We feel that we will be unable to compete globally unless these regulations are amended. Please consider our suggestions carefully.

Best regards



Charles S. Williams  
Chief Scientist  
Cylink Corporation